(19) KOREAN INTELLECTUAL PROPERTY OFFICE

KOREAN PATENT ABSTRACTS

(11)Publication number: 1020000000185 A
(43)Date of publication of application: 15.01.2000

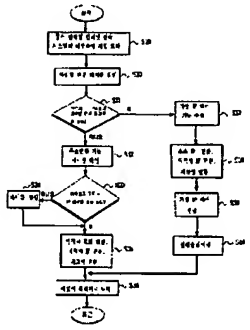
(21)Application number: 1019990041820
(22)Date of filing: 29.09.1999

(51)Int. Cl H04L 12/28

(71)Applicant: CHOI, MYUNG RYUL
(72)Inventor: CHAE, HYEON SEOK
CHOI, MYUNG RYUL

(54) ADDRESS SAVING-TYPE INTERNET CONNECTION METHOD USING NETWORK ADDRESS TRANSLATION(NAT) AND VIRTUAL PRIVATE NETWORK(VPN) CONFIGURATION METHOD

(57) Abstract:



PURPOSE: Address saving-type internet connection method using a network address translation(NAT) saves a IP address, embodies a private network with a single IP address, and easily configures various networks. A virtual private network(VPN) configuration method configures a virtual private network, reduces a cost for the virtual private network(VPN) by using IP address saving-type internet connection method, solves a speed problem without a coding and a preservation protocol, and utilizes all conventional public networks.

CONSTITUTION: When constructing a plurality of servers such as Web, mail, FTP, and tel-net in order to construct a private network, an internet connection system(address translation function router; 10) constructs a virtual private network about a plurality of personal computers and servers to be connected to a hub is constructed with a single IP address, therefore, the number of IP addresses is reduced in constructing a network or a server. When embodying the virtual private network (VPN), a conventional public network can be maximally utilized without regard to any service company, a construction cost of the VPN and a maintenance cost of the VPN can be reduced. A load of a network device is reduced without using a preservation protocol and a coding algorithm, and a preservation maintenance of the VPN is possible.



Legal Status
Date of final disposal of an application (20020226)
Patent registration number (1003335300000)
Date of registration (20020409)
Date of opposition against the grant of a patent (00000000)

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[6]
H04L 12/28

(11) 공개번호 특2000-0000185
(43) 공개일자 2000년01월15일

(21) 출원번호 10-1999-0041820
(22) 출원일자 1999년09월29일

(71) 출원인 최명렬
서울특별시 송파구 잠실본동 320번지 우성4차아파트 103동 602호
(72) 발명자 최명렬
서울특별시 송파구 잠실본동 320번지 우성4차아파트 103동 602호
채현석
경기도안양시동안구관양동한가람마을한양@304동1701호
(74) 대리인 임재룡

*실사청구 : 있음*

# (54) 네트워크 주소 변환(NAT) 기능을 이용한 주소 절약형인터넷 접속 및 가상 사설망(VPN) 구성 방법

*요약*

본 발명은 네트워크 주소 변환(NAT) 기능을 이용한 주소 절약형 인터넷 접속 및 가상 사설망(VPN) 구성 방법에 관한 것이다. 사설망을 구축하기 위해 웹, 메일, FTP, 텔넷 등의 서버들을 구축할 경우 확장된 네트워크 주소 변환(NAT) 기능을 테이블을 포함한 주소 절약형 인터넷 접속 시스템(주소변환 기능 라우터:NAT 라우터)(10)을 사용하여 허브와 연결될 다수 개의 PC와 각종 서버들을 단일 IP 주소 만으로도 가상 사설망을 구성하여 네트워크나 서버 구축시 공인된 IP 주소를 절약하고, 가상 사설망(VPN)을 구현할 경우 어떠한 서비스 업체에 구애받지 않고도 기존의 공개망을 최대한 활용할 수 있고, 가상 사설망의 구축 및 유지 비용을 줄이고 보안 프로토콜이나 암호화 알고리즘이 필요없어 네트워크 장비의 부담을 줄이며 가상 사설망의 보안을 유지할 수 있다.

*대표도*

*도9a*

*색인어*

네트워크 주소 변환(NAT), IP 주소, 절약, 라우터, 가상 사설망(VPN)

*명세서*

*도면의 간단한 설명*

도 1은 종래의 주소 변환 기능 구성도.

도 2a 내지 2b는 종래의 주소 변환 기능을 설명한 흐름도.

도 3은 종래의 가상 사설망(VPN) 구성도.

도 4는 본 발명을 실시하기 위한 주소 절약형 인터넷 접속 시스템 개념도.

도 5a 내지 도 5b는 본 발명에 의한 주소 절약형 인터넷 접속 시스템의 흐름도.

도 6은 본 발명의 일 실시예에 의한 주소 절약형 인터넷 접속 방법을 이용한 가상 사설망(VPN) 구성도.

도 7은 확장된 네트워크 주소 변환(NAT) 기능의 흐름도.

도 8은 NAT(Network Address Translation) 개념도.

도 9a와 도 9b는 본 발명에 의한 가상 사설망(VPN)의 동작을 설명한 흐름도.

* 도면의 주요 부분에 대한 부호 설명 *

8 : 외부 사용자 PC 9 : 인터넷 접속부

10 : 주소 절약형 인터넷 접속 시스템 11: 허브(Hub)

12 : 개인용 PC 13 : 서버(Server)

NAT : 네트워크 주소 변환(Network Address Translation)

VPN : 가상 사설망(Virtual Private Network)

## *발명의 상세한 설명*

### *발명의 목적*

#### *발명이 속하는 기술분야 및 그 분야의 종래기술*

본 발명은 네트워크 주소 변환(Network Address Translation:NAT) 기능을 이용한 주소 절약형 인터넷 접속 및 가상 사설망(Virtual Private Network:VPN) 구성 방법에 관한 것으로써, 특히 가상 사설망(VPN)의 내부에 웹, 메일, FTP, 텔넷 등의 서버들을 구축할 경우 하나의 IP(Internet Protocol) 주소를 가지고도 이러한 서버들을 모두 둘 수 있어 IP 주소를 절약할 수 있으며, 가상 사설망(VPN)을 구현할 경우 어떠한 서비스 업체에 구애받지 않고도 기존의 공개망(Public Network)을 최대한 활용할 수 있으며 보안 프로토콜이나 암호화 알고리즘을 생략하고도 보안을 유지할 수 있는 네트워크 주소 변환(NAT) 기능을 이용한 주소 절약형 인터넷 접속 및 가상 사설망(VPN) 구성 방법에 관한 것이다.

지난 수년 동안 인터넷(Internet)은 급속하게 성장하여 오늘날은 하루에도 상상하기 힘들 정도로 많은 수의 호스트가 인터넷에 연결되고 있으며, 인터넷을 사용하려면 공인된 고유 IP(Internet Protocol) 주소가 호스트에 할당되어야 한다.

그러나, 현재 사용중인 IPv4 타입의 인터넷의 구조는 인터넷 사용 호스트의 점차 증가하고 인터넷 관련 소프트웨어 산업이 발전함에 따라 인터넷에 새롭게 연결되는 모든 호스트들에게 고유한 IP 주소를 제공할 경우 IP 주소 고갈이라는 문제를 야기하게 된다. 이러한 IPv4의 제한을 극복하고자 IP 주소 필드 길이가 대폭 확장되는 IPv6 이라 불리는 새로운 인터넷 프로토콜이 진행 중에 있다.

그러나, 이러한 인터넷 주소 체계에 대한 IPv6 등의 신 표준안을 인터넷에 실제로 적용하고 운영하기에는 많은 어려운 문제들이 남아 있다.

도 1은 종래의 주소 변환 기능 구성도이다.

기존의 주소 변환 기능은 첨부한 도 1과 도 2에서 상세히 설명한다.

도 1을 참조하면, 상기 주소 변환 기능을 이용하는 사설망은 단일 IP 주소와 주소 변환 기능을 가진 라우터(Router), 컴퓨터와 허브(Hub)로 이루어지며, 웹 서버, 메일 서버, FTP 서버, 텔넷 서버 등의 서버 구축시에는 서버 개수만큼 별도의 IP 주소가 있어야 한다.

도 2a 내지 2b는 종래의 주소 변환 기능을 설명한 흐름도이다.

도 2a를 참조하면, IP 패킷이 주소 변환 기능 라우터의 내부쪽으로 들어오면(단계 S1), 주소변환 기능 테이블을 확인하고(단계 S2) 상기 IP 패킷의 소스 포트(source port)와 다음 표 1에 도시한 바와 같이 주소 변환 기능 테이블의 포트(port)를 비교하여(단계 S3), 상기 주소변환 기능 테이블에 있으면 테이블을 참고하여 소스 포트와 소스 IP를 바꾸고 체크섬(check sum)을 바꾼(단계 S5) 후 IP 패킷이 목적지에 도착한다(단계 S6).

S3 단계에서 IP 패킷의 소스 포트(source port)가 상기 주소변환 기능 테이블에 없으면, 즉 주소변환 기능 테이블의 포트와 IP 패킷의 소스 포트가 같지 않으면 새로운 주소변환 기능 테이블을 생성한(단계 S4) 후, 그 테이블을 참고하여 소스 포트와 소스 IP를 바꾸고 체크섬을 바꾼다(단계 S5).

*[표 1]*

| 테이블 | | |
|---|---|---|
| 내부 IP 주소 | 포트 | 로컬 주소 변환 기능 포트 |
| 10.1.1.2 | 1111 | 2222 |
| | 3112 | 2223 |
| 10.1.5.48 | : | : |
| : | | |

도 2b를 참조하면, IP 패킷이 주소변환 기능 라우터의 외부쪽으로 들어오면(단계 S7) 상기 주소변환 기능 테이블을 확인하고(단계 S8) IP 패킷의 목적지 포트(destination port)와 IP 패킷의 목적지 포트와 상기 주소변환 기능 테이블의 로컬(local) 주소변환 기능 포트를 비교하여(단계 S9), 상기 주소변환 기능 테이블에 있으면 상기 주소변환 기능 테이블을 참고하여 목적지 포트(destination port)와 목적지 IP를 바꾸고, 체크섬(check sum)을 변환(단계 S11) 후 IP 패킷이 목적지에 도달한다(단계 S12).

S9 단계에서 IP 패킷의 목적지 포트가 상기 주소변환 기능 테이블에 없으면 그 패킷은 폐기한다(단계 S10).

네트워크 주소 변환(Network Address Translation:NAT)은 주소 할당 메카니즘을 이용하여 사설망(Private Network)의 IP 주소를 글로벌망(Global Network)의 IP 주소를 변환시키는 기능으로써, 라우터나 방화벽(Firewall) 등에 내장되어 IP 주소를 절약하는 데 사용된다.

최근, 인터넷 방 등을 비롯한 소호(SOHO:Small Pffice Home Office) 환경의 인터넷 사용자들이 늘어나면서 이러한 NAT 기능의 중요성은 점점 증가하고 있다.

그러나, 이러한 NAT(Network Address Translation) 기능은 외부 망으로부터 접근이 불가능하다는 특성을 가지고 있어 보안 유지 측면에서는 장점으로 작용하나, 소규모 기업이나 사무실이 웹 서버(Web server)나 메일 서버 등을 두고 싶어하는 경우에는 외부에서의 접근이 허용되어야 하므로 단점이 된다. 그리하여 웹이나 메일 등의 서버 구축을 위해서는 이러한 서버를 NAT 기능의 외부에 설치하거나 인터넷 서비스 업체의 서비스를 받아야한다. 이렇게 되면 사용해야할 IP 주소가 증가하게 되거나 서비스 업체로 들어가는 비용이 추가로 발생하게 된다.

도 3을 참조하면, 종래의 가상 사설망(Virtual Private Network:VPN)은 전용선을 구축해 놓은 인터넷 서비스 제공업체와 그 인터넷 서비스 제공업체의 POP(Point Of Presence)까지 연결하는 WAN, 그리고 기업의 사설망으로 이루어진다.

상기 가상 사설망의 동작은 전용선을 구축해 놓고 보안 프로토콜을 제공하는 인터넷 서비스 제공업체로부터 서비스를 받으며, 자사와 가장 가까운 인터넷 서비스 제공업체의 POP(Point of Presence)까지 WAN으로 연결하고, 재택 근무, 출장 직원, 현장 엔지니어들은 가까운 인터넷 서비스 제공업체의 POP에 전화 접속으로 연결한 후, 인터넷을 통해 홈 네트워크를 이용하며 보안 프로토콜도 일정하다는 단점을 보완하기 위해 암호화 알고리즘을 사용하여 패킷을 전송한다.

그러나, 종래의 주소 변환 기능 기술의 문제점은 첫째, 기존의 주소 변환 기능은 IP 주소를 절약하는 데 도움이 되기는 했으나 서버를 추가로 구축할 경우 IP 주소를 더 받아야하는 문제가 있으며, 둘째 이러한 서버 구축시 추가되는 IP 주소 때문에 유지비용이 더 증가하는 단점이 있었다.

종래의 가상 사설망 기술의 문제점은 보안을 위해 매우 복잡한 알고리즘을 수행하여 네트워크 장비에 부담을 주고 속도가 느려지는 문제가 있으며, 장비가격이 높아지며, 가상 사설망(VPN)이 보안 프로토콜을 사용하여 구성되어야 하는 등 인터넷 서비스 업체에게 전적으로 의존해야 했으며, 가상 사설망의 유지 비용이 증가하면서도 보안문제에 완벽하지 않다는 문제가 있었으며, 가상 사설망 기술을 사용하는 데 있어서 공개망의 일부만 사용할 수 있다는 한계가 있는 문제점이 있다.

### *발명이 이루고자 하는 기술적 과제*

본 발명은 상기한 종래 기술의 문제점을 해결하기 위해 제안된 것으로써, 본 발명의 목적은 IPv4의 주소가 부족한 상황에서 IP 주소를 절약하고 각종 서버를 포함하면서도 단일 IP 주소만으로 사설망을 구축할 수 있고 단일 IP 주소만으로 다양한 망 구성을 쉽고 저렴하게 할 수 있는 네트워크 주소 변환(NAT) 기능을 이용한 주소 절약형 인터넷 접속 방법과, 인터넷 서비스 제공업체의 서비스를 받지 않고도 원하는 대로 가상 사설망을 구성하고, IP 주소 절약형 인터넷 접속 방법을 이용하여 가상 사설망(VPN)의 구축 및 유지비용을 줄이며 암호화나 보안 프로토콜이 필요없어 네트워크 장비에 부담이 적고 속도 문제가 해결되어 기존의 공개망을 모두 활용할 수 있는 IP 주소 절약형 인터넷 접속 방법을 이용한 가상 사설망(VPN)을 구성하고, 주소 할당 메카니즘을 이용하여 사설망(Private Network)의 IP 주소를 글로벌망(Global Network) IP 주소로 변환시켜주는 기능인 네트워크 주소 변환(Network Address Translation:NAT)을 사용하여 라우터나 방화벽(Firewall) 등에 내장되어 특히 IP 주소의 절약을 목적으로 사용되는 네트워크 주소 변환(NAT) 기능을 이용한 주소 절약형 인터넷 접속 및 가상 사설망(Virtual Private Network:VPN) 구성 방법을 제공한다.

### *발명의 구성 및 작용*

상기한 목적을 달성하기 위해 본 발명은 인터넷 접속부(9), 주소 절약형 인터넷 접속 시스템(NAT 라우터:주소 변환 기능 라우터)(10), 허브(Hub)(11), 개인용 PC(12) 및 각종 서버(13)를 구비한 네트워크 시스템에 있어서, (a) IP 패킷이 주소 절약형 인터넷 접속 방법을 이용하여 구축한 가상 사설망(VPN)의 상기 주소 절약형 인터넷 접속 시스템의 내부에 도착하면(S29), 사설망 연결 테이블을 확인하고(S30), IP 패킷의 목적지 IP 주소가 상기 사설망 연결 테이블에 등록된 주소인지 확인하는 단계(S31); (b) S31 단계에서 패킷의 목적지 IP 주소가 상기 사설망 연결 테이블에 등록된 주소라면 가상 IP 헤더 기능을 수행하기 시작하고(S37), 목적지 포트(destination port) 변환, 목적지 IP 변환, 체크섬(check sum)을 변환하여(S38) 상기 사설망 연결 테이블에서 목적지 IP 주소를 얻고 상기 주소 변환 기능 라우터(10)에서 발신지 IP 주소를 얻어 이것으로 가상의 IP 헤더를 생성한(S39) 후 생성한 헤더를 원래의 사설망간 IP 패킷에 인캡슐레이션(encapsulation)하고(S40) 패킷이 목적지로 도착하는 단계(S36); (c) S31 단계에서 패킷의 목적지 IP 주소가 상기 사설망 연결 테이블에 등록된 주소가 아니라면 주소 절약형 인터넷 접속 시스템의 상기 주소변환 기능 테이블(NAT 테이블)을 확인하고(S32), 상기 주소변환 기능 테이블의 포트가 IP 패킷의 소스 포트와 동일한지를 체크하여(S33) 상기 주소변환 테이블의 생성하고(S34), 소스 포트(source port) 변환, 소스 IP 변환, 체크섬 변환한(S35) 후 패킷이 목적지로 도착하는 단계(S36); (d) 보내진 IP 패킷이 주소 절약형 인터넷 접속 방법을 이용하여 구축한 가상 사설망(VPN)의 상기 주소 절약형 인터넷 접속 시스템의 외부에 도착하면(S41), 사설망 연결 테이블을 확인하고(S42), IP 패킷의 소스 IP 주소가 상기 사설망 연결 테이블에 등록된 주소인지 확인하는 단계(S43); (e) S43 단계에서 패킷의 소스 IP 주소가 상기 사설망 연결 테이블에 등록된 주소라면 가상 IP 헤더 기능을 수행하기 시작하여(S48) 가상 IP 헤더를 삭제하고(S49) 이 가상 IP 헤더가 원래의 사설망간 IP 패킷이 목적지에 도착하는 단계(S50); 및 (f) S43 단계에서 패킷의 소스 IP 주소가 상기 사설망 연결 테이블에 등록된 주소가 아니라면 주소 절약형 인터넷 접속 시스템의 상기 주소변환 기능 테이블(NAT 테이블)을 확인하고(S44) 상기 주소변환 기능 테이블의 로컬 주소변환 기능 포트가 IP 패킷의 목적지 포트와 동일한지를 체크하여(S45) 같지 않으면 패킷을 버리고(단계 S46) 같으면 목적지 포트(destinat ion port) 변환, 목적지 IP 변환, 체크섬 변환한(단계 S47) 다음 패킷이 목적지에 도착하는 단계(S50)로 구성되는 것을 특징으로 하는 네트워크 주소 변환(NAT) 기능을 이용한 주소 절약형 인터넷 접속 및 가상 사설망(VPN) 구성 방법을 제공한다.

본 발명에서는 이러한 단점을 극복하기 위하여 NAT 테이블(NAT table)에 수정을 가함으로써 사설망 내부

의 특정 서버에 접근할 수 있는 확장된 개념의 NAT를 제안한다. 확장된 NAT 기능은 서비스 별로 한 개씩의 서버를 지정할 수 있으며, 이러한 특정 서버로의 접속 이외의 접속은 금하면서 외부에 알리고 싶은 서버는 내부에 둘 수 있게 된다. 결국, 원하는 기능은 수행하면서 NAT IP 주소는 단일 IP로도 운영이 가능하다.

이하, 첨부한 도면을 참조하여 본 발명에 따른 바람직한 실시예를 상세하게 설명한다.

도 4는 본 발명을 실시하기 위한 주소 절약형 인터넷 접속 시스템 구성도이다. 도 4를 참조하면, IP 주소 절약형 인터넷 접속 방법을 이용한 사설망은 단일 IP 주소와 주소 절약형 인터넷 접속 시스템의 테이블이 포함된 라우터인 주소 절약형 인터넷 접속 시스템(10), 외부 사용자 PC(8), 인터넷 접속부(9), 허브(Hub)(11), 개인용 PC(12) 및 서버(Server)(13)로 구성된다.

상기 인터넷 접속부(9)는 모뎀을 이용한 전화망 혹은 DSU 또는 CSU 등을 이용하는 전용선, LAN, xDSL, FTTH(Fiber To The Home)등이 된다.

이하, 주소 변환 기능을 이용한 주소 절약형 인터넷 접속 방법은 도 5a, 도 5b, 도 6에서 설명한다. 도 5a 내지 도 5b는 본 발명에 의한 주소 절약형 인터넷 접속 시스템의 흐름도이다.

도 5b를 참조하면, 접속을 원하는 서버의 포트와 IP 주소를 주소 절약형 인터넷 접속 시스템(NAT 라우터)의 주소변환 기능 테이블(표2)에 미리 등록하고, IP 패킷이 주소 변환 기능 라우터의 외부쪽으로 들어오면(단계 S22) 주소 절약형 인터넷 접속 시스템의 주소변환 기능 테이블을 확인하고(단계 S23), IP 패킷의 목적지 포트(destination port)와 상기 주소변환 기능 테이블의 로컬 주소 변환 기능 포트를 비교하여(단계 S24), 그 포트가 주소변환 기능 테이블에 정의되어 있으면 IP 패킷은 주소변환 기능 테이블을 참고하여 목적지 포트와 목적지 IP를 바꾸고, 체크섬(check sum)을 바꾼(단계 S26) 후 패킷이 목적지인 서버에 접속된다(단계 S27). S24 단계에서 IP 패킷의 목적지 포트가 상기 주소변환 기능 테이블에 없으면 패킷을 폐기한다(단계 S25).

도 5a를 참조하면, IP 패킷이 주소 변환 기능 라우터(NAT 라우터)의 내부쪽으로 들어오면(단계 S16) 주소 절약형 인터넷 접속 시스템의 주소변환 기능 테이블을 확인하여(단계 S17), 패킷의 소스 포트(source port)와 상기 주소변환 기능 테이블(표 2)의 포트를 비교하여(단계 S18), 상기 주소 변환 기능 테이블에 있으면 상기 테이블을 참고하여 소스 포트(source port)와 소스 IP를 바꾸고, 체크섬(check sum)을 바꾼(단계 S19) 후, 패킷이 목적지에 도착한다(단계 S21). 상기 주소변환 기능 테이블에 없으면 새로운 테이블을 생성한(단계 S20) 후 그 테이블을 참고하여 소스 포트와 소스 IP를 바꾸고 체크섬을 바꾼다.

본 발명에서 제안하는 확장된(Network Address Translation:NAT) 기능의 동작의 핵심은 NAT 테이블에 대한 수정을 가함으로써 우리가 원하는 특정 서버에 연결 요구시 이를 적절히 처리하는 것이다.

상술한 NAT 방식을 보면 알 수 있듯이, NAT 라우터의 외부 쪽으로 들어오는 패킷은 수신처 포트 번호와 테이블의 로컬(local) NAT 포트 번호를 비교하여 같은 것이 있을 때에만 그에 관련된 데이터를 참고하여 들어올 수 있다.

그리고, 우리가 NAT 내부에 달고 싶어하는 서버는 특정한 몇 종류 뿐이다. 그러므로, 우리는 원하는 웹이나 메일, 텔넷(telnet) 등의 서버에 관련된 포트 번호(참고, FTP의 포트 번호:21, 텔넷의 포트 번호:23, 메일의 포트 번호:25, 웹 서버의 포트번호:80)를 NAT 테이블의 로컬 NAT 포트 번호로 고정시켜 둔다면 그러한 특정 서버를 목적하는 패킷은 들어올 수 있을 것이다. 물론 기존의 네트워크 주소 변환(NAT) 기능은 그대로 수행한다.

다음은 NAT 내부에 두기를 원하는 서버의 포트 번호를 고정시켜 놓은, 확장된 NAT 테이블의 예이다.

*[표 2]*

| 테이블 | | |
|---|---|---|
| 내부 IP 주소 | 포트 | 로컬 주소 변환 기능 포트 |
| 10.1.1.2 | 23 | 23 |
| | 80 | 80 |
| 10.1.5.48 | : | : |
| : | | |

확장된 NAT(Network Address Translation) 방식을 사용할 때, 운영자가 NAT 라우터에 텔넷(telnet)으로 접속하고 싶을 때는 포트 번호(23)가 겹치는 문제가 발생할 수 있으나, 이것은 운영자만이 쓰는 것이므로 그 만이 쓸 포트 번호로 바꾸어 쓰도록 한다면 해결될 것이다.

이하 도6과 도 7을 참조하여 주소 절약형 인터넷 접속 방법을 이용한 가상 사설망 (Virtual Private Network:VPN) 구성 방법을 설명한다.

도 6은 본 발명의 일 실시예에 의한 주소 절약형 인터넷 접속 방법을 이용한 가상 사설망(VPN) 구성도이다.

도 6을 참조하면, 본 발명에 의한 주소 절약형 인터넷 접속 기법을 이용한 가상 사설망(VPN)은 주소 절약형 인터넷 접속 방법으로 이루어진 사설망(10.1.100.X)과 이러한 사설망(10.1.200.X)간의 연결을 위한 상기 주소 절약형 인터넷 접속 시스템(10)에 각각 내재된 사설망 연결 테이블로 이루어지어 상기 주소 공인

된 두 개의 IP 주소(200.1.1.1과 210.1.1.1)를 통해 가상 사설망간의 IP 주소를 절약하여 데이터를 송수신할 수 있다.

확장된 NAT 테이블을 이용하여 사설망 외부에 있는 호스트2에서부터 내부에 있는 호스트1 으로 접속이 이루어지는 과정을 도 7에서 상세히 설명한다.

도 7은 확장된 네트워크 주소 변환(NAT) 기능의 흐름도이다.

도 7을 참조하면, IP 패킷이 NAT 라우터의 외부쪽으로 들어올 때(①), 패킷의 수신처 포트 번호와 NAT 테이블의 로컬 NAT 포트 번호를 비교하여 그 포트 번호가 NAT 테이블에 정의되어 있으면(예를 들어 텔넷의 포트 번호 23) 상기 NAT테이블을 참고하여 수신처 포트 번호를 바꾸고(23->23)(여기서 앞의 23은 텔넷 포트번호를 의미하고, 뒤의 23은 고정된 포트 번호를 의미) 수신처 IP 주소를 바꾸고(166.104.226.104), 체크섬(check sum)을 바꾼다(②). 만약, 상기 NAT 테이블에 없으면 패킷은 버린다. 그런 후, 패킷은 목적지인 호스트1에 도착한다(③). 그리하여 받은 패킷에 대한 응답 패킷(받은 패킷에서 수신처 주소와 발신원 주소의 위치를 바꾸고, 수신처 포트 번호와 발신원 포트 번호의 위치를 바꿈)이 NAT 라우터의 내부쪽으로 들어오면(④), 패킷의 발신원 포트 번호와 NAT 테이블의 포트 번호를 비교하여 상기 NAT 테이블에 있으면 상기 NAT 테이블을 참고하여 발신원 포트 번호를 바꾸고(23->23), 발신원 IP 주소를 바꾸고(10.1.1.2->166.104.226.104), 체크 섬을 바꾼다(⑤). 만약 NAT 테이블에 없으면 기존의 네트워크 주소 변환(NAT)처럼 테이블을 새로이 생성한다. 패킷이 목적지인 호스트2에 도착한다(⑥).

이러한 도 8의 NAT 개념도를 참조하여 확장된 NAT에서의 패킷의 변화는 표 3에 자세히 표시하였다.

*[표 3]*

| | 수신처 주소 | 발신원 주소 | 수신처 포트번호 | 발신원 포트번호 | … |
|---|---|---|---|---|---|
| ① | 166.104.226.104 | 138.201.148.165 | 23 | 1111 | … |
| ② | 10.1.1.2 | 138.201.148.165 | 23 | 1111 | … |
| ④ | 138.201.148.165 | 10.1.1.2 | 1111 | 23 | … |
| ⑤ | 138.201.148.165 | 166.104.202.104 | 1111 | 23 | … |

도 9a와 9b는 본 발명에 의한 가상 사설망(VPN)의 동작을 설명한 흐름도이다. 도 9a를 참조하면, 인터넷 접속부(9), 주소 절약형 인터넷 접속 시스템(NAT 라우터:주소 변환 기능 라우터)(10), 허브(Hub)(11), 개인용 PC(12) 및 각종 서버(13)를 구비한 네트워크 시스템에 있어서, IP 패킷이 주소 절약형 인터넷 접속 방법을 이용하여 구축한 가상 사설망(VPN)의 상기 주소 절약형 인터넷 접속 시스템의 내부에 도착하면(단계 S29), 사설망 연결 테이블을 확인하고(단계 S30), IP 패킷의 목적지 IP 주소가 상기 사설망 연결 테이블에 등록된 주소인지 확인한다(단계 S31).

S31 단계에서 패킷의 목적지 IP 주소가 상기 사설망 연결 테이블에 등록된 주소라면 가상 IP 헤더 기능을 수행하기 시작하고(단계 S37), 목적지 포트(destination port) 변환, 목적지 IP 변환, 체크섬(check sum)을 변환하여(단계 S38) 상기 사설망 연결 테이블에서 목적지 IP 주소를 얻고 상기 주소 변환 기능 라우터(10)에서 발신지 IP 주소를 얻어 이것으로 가상의 IP 헤더를 생성한(단계 S39) 후 생성한 헤더를 원래의 사설망간 IP 패킷에 인캡슐레이션(encapsulation)하고(단계 S40) 패킷이 목적지로 도착한다(단계 S36).

S31 단계에서 패킷의 목적지 IP 주소가 상기 사설망 연결 테이블에 등록된 주소가 아니라면 주소 절약형 인터넷 접속 시스템의 상기 주소변환 기능 테이블(NAT 테이블)을 확인하고(단계 S32), 상기 주소변환 기능 테이블의 포트가 IP 패킷의 소스 포트와 동일한지를 체크하여(단계 S33) 상기 주소변환 테이블의 생성하고(단계 S34), 소스 포트(source port) 변환, 소스 IP 변환, 체크섬 변환한(단계 S35) 후 패킷이 목적지로 도착한다(단계 S36).

도 9b를 참조하면, 위의 도 9a에서 보내진 IP 패킷이 주소 절약형 인터넷 접속 방법을 이용하여 구축한 가상 사설망(VPN)의 상기 주소 절약형 인터넷 접속 시스템의 외부에 도착하면(단계 S41), 사설망 연결 테이블을 확인하고(단계 S42), IP 패킷의 소스 IP 주소가 상기 사설망 연결 테이블에 등록된 주소인지 확인한다(단계 S43).

S43 단계에서 패킷의 소스 IP 주소가 상기 사설망 연결 테이블에 등록된 주소라면 가상 IP 헤더 기능을 수행하기 시작하여(단계 S48) 가상 IP 헤더를 삭제하고(단계 S49) 이 가상 IP 헤더가 원래의 사설망간 IP 패킷이 목적지에 도착한다(단계 S50).

S43 단계에서 패킷의 소스 IP 주소가 상기 사설망 연결 테이블에 등록된 주소가 아니라면 주소 절약형 인터넷 접속 시스템의 상기 주소변환 기능 테이블(NAT 테이블)을 확인하고(단계 S44) 상기 주소변환 기능 테이블의 로컬 주소변환 기능 포트가 IP 패킷의 목적지 포트와 동일한지를 체크하여(단계 S45) 같지 않으면 패킷을 버리고(단계 S46) 같으면 목적지 포트(destination port) 변환, 목적지 IP 변환, 체크섬 변환한(단계 S47) 다음 패킷이 목적지에 도착한다(단계 S50).

네트워크 주소 변환(Network Address Translation:NAT)이 처음 개발될 당시에는 단지 IP 주소 고갈 문제에 대한 대안으로만 생각되었을 뿐, 그 누구도 완전히 다른 영역에서도 유용할 거라고는 생각하지 않았다. 그러나, NAT 기능은 인터넷 환경이 IPv6으로 변화되더라도, 보안이나 IP 주소 할당의 편리성을 이유로 계속 사용될 것이고, 여러 영역에서 적용될 것으로 보인다. 최근 점점 복잡하고 다양한 형태의 인터넷 접속이 요구되면서 NAT 기능은 필수적인 기능이 되고 있으나, 외부로부터의 접속이 전혀 불가능함으로써 극히 제한적으로 사용되고 있다.

본 발명에서 제안된 확장된 NAT 기능은 이러한 단점을 극복할 수 있는 간단하면서도 매우 유용한 방법으로써, 향후 많은 적용이 이루어지리라 사료된다. 현재 인터넷 구성이 핵심 장비인 라우터(router)나 방화

벽(Firewall) 등에 쉽게 적용이 가능하며, 망 관리 방법 또한 매우 용이하게 이루어 질 것으로 사료된다. 특히 앞으로의 그 사용 형태를 예측하기 힘들 정도로 다양한 형태를 보이고 있는 소호(SOHO) 사용자들이 다양한 요구를 수용하는 가상 사설망(VPN) 구성시 적절히 사용할 수 있을 것이다.

### *발명의 효과*

상술한 바와 같이, 본 발명에 의한 네트워크 주소 변환(NAT) 기능을 이용한 주소 절약형 인터넷 접속 및 가상 사설망(VPN) 구성 방법은 네트워크 주소 변환(NAT) 기능을 이용한 주소 절약형 인터넷 접속 방법을 사용함에 따라 IP 주소가 부족한 현 상황에서 IP 주소를 절약할 수 있고, 단일 IP 주소로 사설망 내에 종류별로 서버를 구축할 수 있으며 단일 IP 주소로도 다양한 망 구성을 쉽고 저렴하게 할 수 있으며, 주소 절약형 인터넷 접속 방법을 이용한 가상 사설망 구성 방법을 사용함에 따라 인터넷 서비스 제공업체가 필요없는 방법으로 가상 사설망 구축과 유지에 들어가는 비용을 많이 줄이고, 인터넷 서비스 제공업체 없이도 기존 공개망을 최대한 활용하여 가상 사설망(VPN)을 구성할 수 있으며, 보안 프로토콜이나 암호화 알고리즘 없이도 보안문제를 해결함에 의해 네트워크 장비의 부담이 줄이고 처리속도가 빨라지게 하는 효과가 있다.

상기에서는 본 발명의 바람직한 실시 예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

### *(57) 청구의 범위*

#### 청구항 1

인터넷 접속부(9), 주소 절약형 인터넷 접속 시스템(NAT 라우터:주소 변환 기능 라우터)(10), 허브(Hub)(11), 개인용 PC(12) 및 각종 서버(13)를 구비한 네트워크 시스템에 있어서,

(a) IP 패킷이 주소 절약형 인터넷 접속 방법을 이용하여 구축한 가상 사설망(VPN)의 상기 주소 절약형 인터넷 접속 시스템의 내부에 도착하면(S29), 사설망 연결 테이블을 확인하고(S30), IP 패킷의 목적지 IP 주소가 상기 사설망 연결 테이블에 등록된 주소인지 확인하는 단계(S31);

(b) S31 단계에서 패킷의 목적지 IP 주소가 상기 사설망 연결 테이블에 등록된 주소라면 가상 IP 헤더 기능을 수행하기 시작하고(S37), 목적지 포트(destination port) 변환, 목적지 IP 변환, 체크섬(check sum)을 변환하여(S38) 상기 사설망 연결 테이블에서 목적지 IP 주소를 얻고 상기 주소 변환 기능 라우터(10)에서 발신지 IP 주소를 얻어 이것으로 가상의 IP 헤더를 생성한(S39) 후 생성한 헤더를 원래의 사설망간 IP 패킷에 인캡슐레이션(encapsulation)하고(S40) 패킷이 목적지로 도착하는 단계(S36);

(c) S31 단계에서 패킷의 목적지 IP 주소가 상기 사설망 연결 테이블에 등록된 주소가 아니라면 주소 절약형 인터넷 접속 시스템의 상기 주소변환 기능 테이블(NAT 테이블)을 확인하고(S32), 상기 주소변환 기능 테이블의 포트가 IP 패킷의 소스 포트와 동일한지를 체크하여(S33) 상기 주소변환 테이블의 생성하고(S34), 소스 포트(source port) 변환, 소스 IP 변환, 체크섬 변환한(S35) 후 패킷이 목적지로 도착하는 단계(S36);

(d) 보내진 IP 패킷이 주소 절약형 인터넷 접속 방법을 이용하여 구축한 가상 사설망(VPN)의 상기 주소 절약형 인터넷 접속 시스템의 외부에 도착하면(S41), 사설망 연결 테이블을 확인하고(S42), IP 패킷의 소스 IP 주소가 상기 사설망 연결 테이블에 등록된 주소인지 확인하는 단계(S43);

(e) S43 단계에서 패킷의 소스 IP 주소가 상기 사설망 연결 테이블에 등록된 주소라면 가상 IP 헤더 기능을 수행하기 시작하여(S48) 가상 IP 헤더를 삭제하고(S49) 이 가상 IP 헤더가 원래의 사설망간 IP 패킷이 목적지에 도착하는 단계(S50); 및

(f) S43 단계에서 패킷의 소스 IP 주소가 상기 사설망 연결 테이블에 등록된 주소가 아니라면 주소 절약형 인터넷 접속 시스템의 상기 주소변환 기능 테이블(NAT 테이블)을 확인하고(S44) 상기 주소변환 기능 테이블의 로컬 주소변환 기능 포트가 IP 패킷의 목적지 포트와 동일한지를 체크하여(S45) 같지 않으면 패킷을 버리고(단계 S46) 같으면 목적지 포트(destination port) 변환, 목적지 IP 변환, 체크섬 변환한(단계 S47) 다음 패킷이 목적지에 도착하는 단계(S50)로 구성되는 것을 특징으로 하는 네트워크 주소 변환(NAT) 기능을 이용한 주소 절약형 인터넷 접속 및 가상 사설망(VPN) 구성 방법.

#### 청구항 2

제 1 항에 있어서,

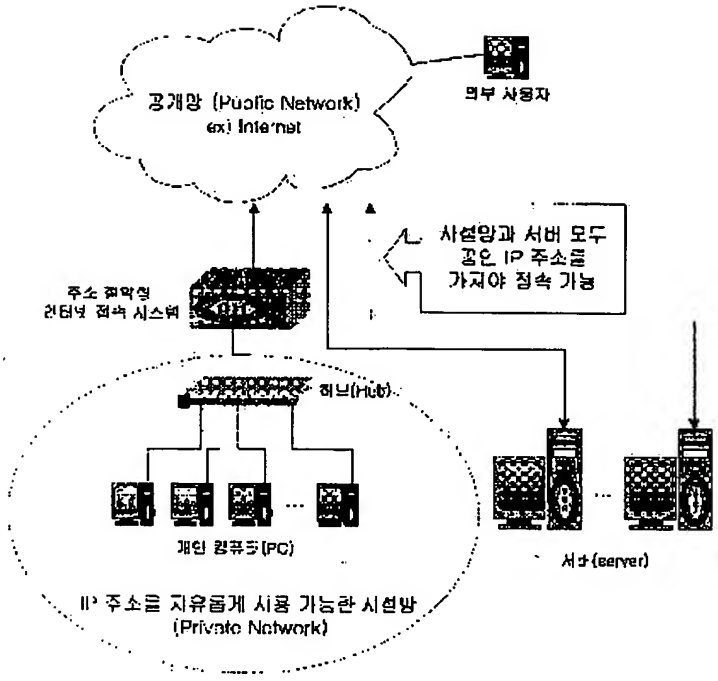
상기 주소 절약형 인터넷 접속 시스템(NAT 라우터)(10)에 내재되는 NAT(Network Address Translation) 테이블에 확장된 NAT 기능을 추가하여 웹 서버, 메일 서버, FTP 서버, 텔넷 서버 등의 각종 서버를 외부에서도 접근 가능하도록 상기 확장된 NAT 테이블에 사설망의 내부 IP주소, 포트 번호, 로컬 NAT 번호를 정의하고, 네트워크나 서버 설치시 IP 주소를 절약하고 각종 서버를 포함하면서도 단일 IP 주소만으로도 IP 주소 절약형 인터넷 접속 방법을 이용하여 여러 형태의 사설망(VPN)을 구축할 수 있으며, 암호화나 보안 프로토콜이 필요 없는 것을 특징으로 하는 네트워크 주소 변환(NAT) 기능을 이용한 주소 절약형 인터넷 접속 및 가상 사설망(VPN) 구성 방법.

#### 청구항 3

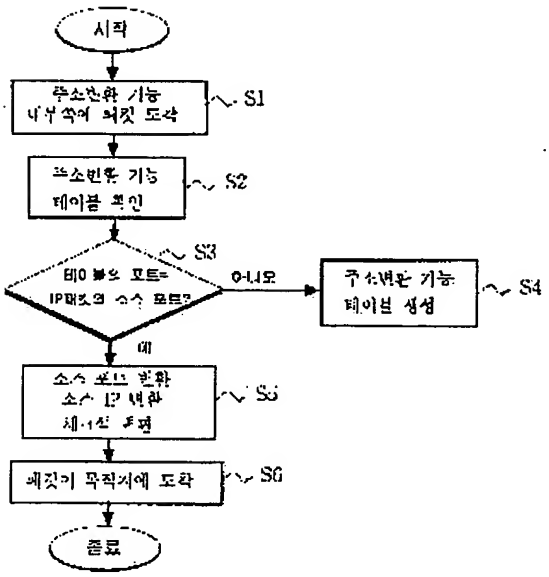
상기 주소 절약형 인터넷 접속 시스템(NAT 라우터)(10)에 상기 가상 사설망(VPN)에서 외부로 IP 패킷을 송신시 제공되는 상기 기능 (a), 상기 기능 (b), 상기 기능 (c)과 외부로부터 상기 가상 사설망(VPN)으로 IP 패킷을 수신시 제공되는 상기 기능 (d), 상기 기능 (e), 상기 기능 (f)를 실현시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체.

도면

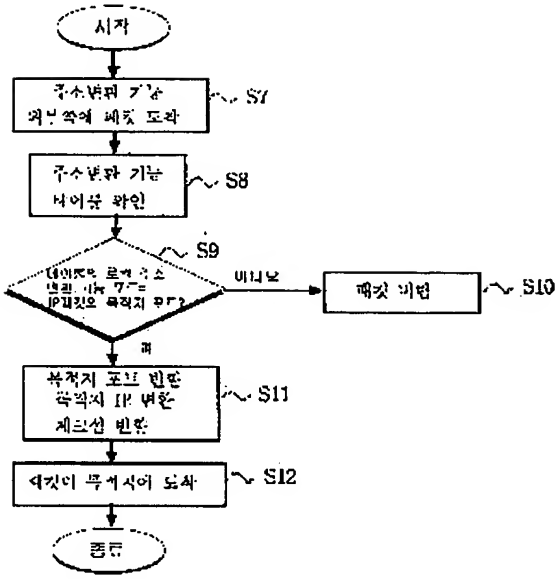
도면1


공개망 (Public Network)
ex) Internet
외부 사용자
사설망과 서버 모두
공인 IP 주소를
가지야 접속 가능
주소 변환형
라우터 접속 시스템
허브(Hub)
개인 컴퓨터(PC)
서버(server)
IP 주소를 자유롭게 사용 가능한 사설망
(Private Network)

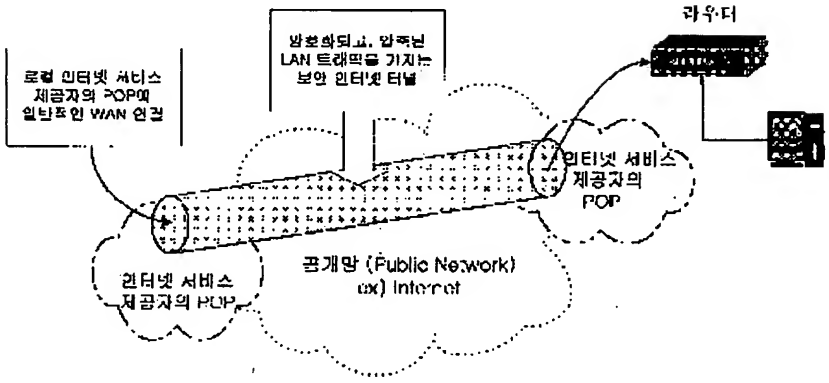
도면2a


시작
주소변환 기능
내부에서 패킷 도착
S1
주소변환 기능
테이블 확인
S2
S3
아니오
주소변환 기능
테이블 생성
S4
예
S5
패킷기 목적지에 도착
S6
종료

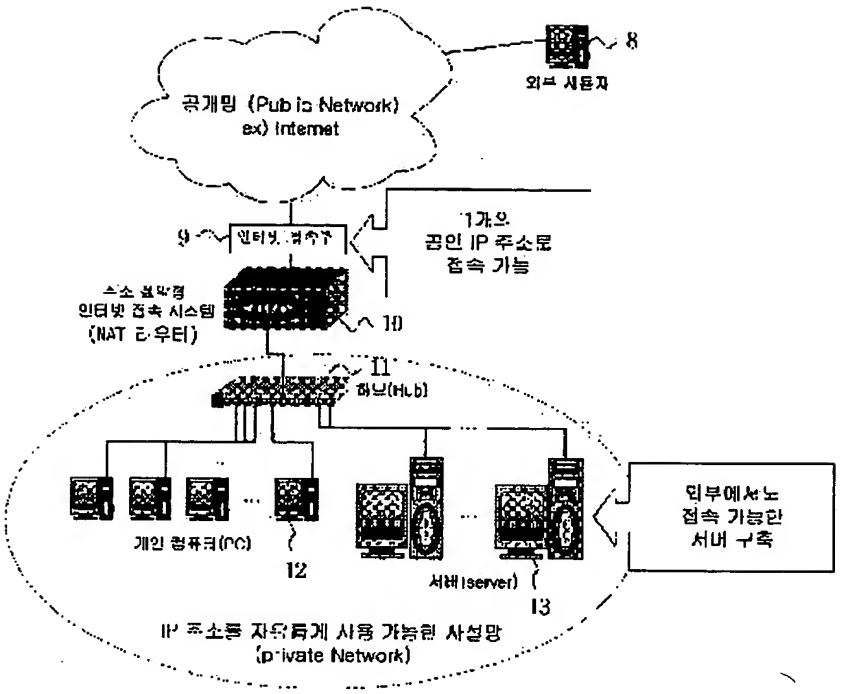
도면2b


시작
S7
S8
S9
아니오
S10
S11
S12
종료

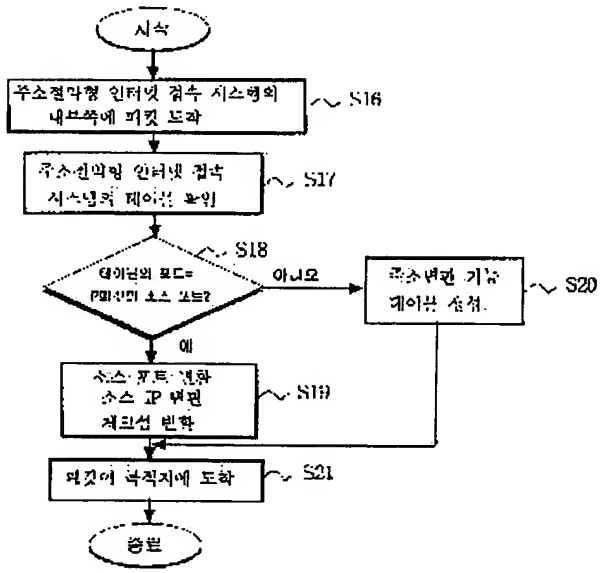
도면3


라우터
암호화되고, 압축된
LAN 트래픽을 가지는
보안 인터넷 터널
로컬 인터넷 서비스
제공자의 POP에
일반적인 WAN 연결
인터넷 서비스
제공자의
POP
공개망 (Public Network)
ex) Internet
인터넷 서비스
제공자의 POP

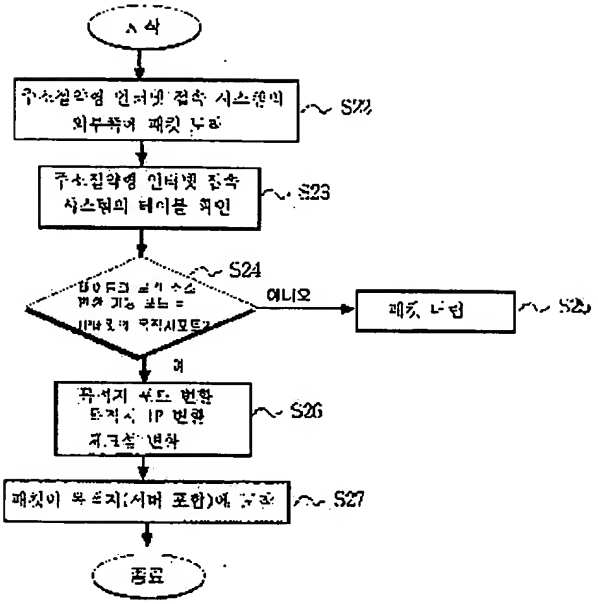
도면4


8
외부 사용자
공개망 (Public Network)
ex) Internet
9
1개의
공인 IP 주소로
접속 가능
10
11
허브(Hub)
개인 컴퓨터(PC)
12
서버(server)
13
내부에서도
접속 가능한
서버 구축
IP 주소를 자유롭게 사용 가능한 사설망
(private Network)

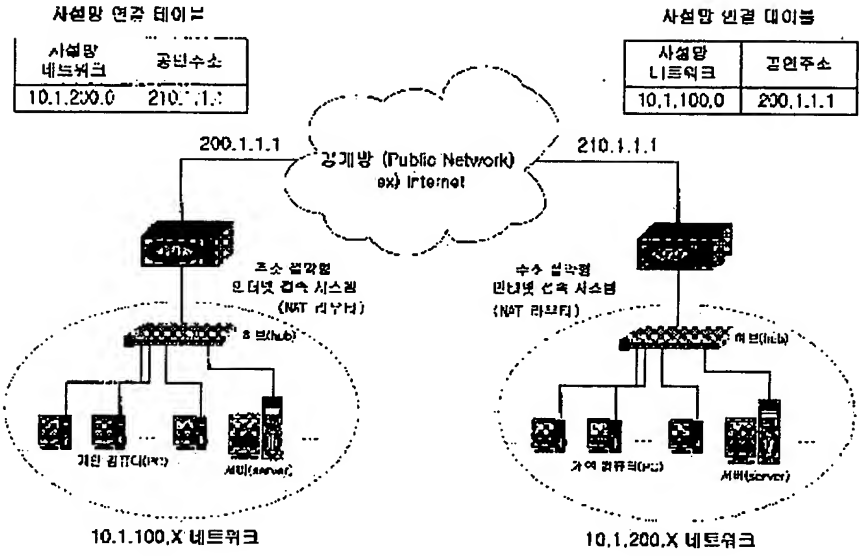
도면5a


시작
S16
S17
S18
아니오
S20
예
S19
S21
종료

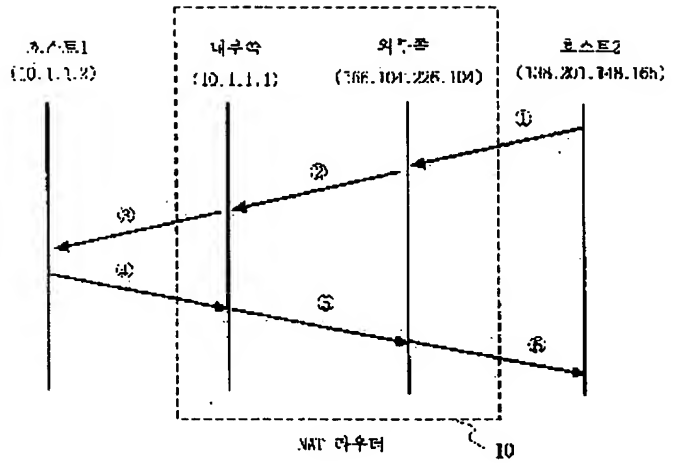
도면5b


시작
S22
S23
S24
아니오
S25
예
S26
S27
종료

도면6

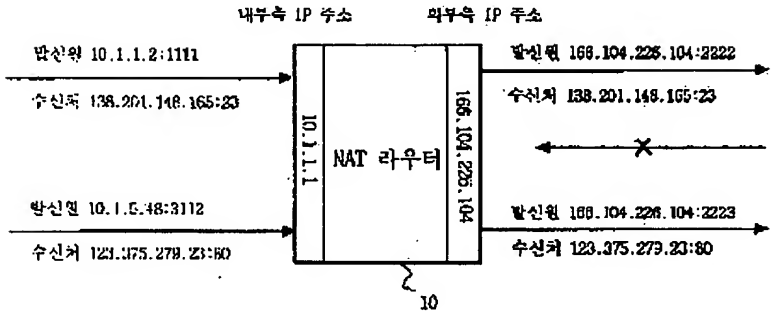

사설망 연결 테이블
사설망 네트워크
공인주소
10.1.200.0
사설망 인결 테이블
사설망 네트워크
공인주소
10.1.100.0
200.1.1.1
200.1.1.1
210.1.1.1
공개망 (Public Network)
ex) Internet
10.1.100.X 네트워크
10.1.200.X 네트워크

도면7

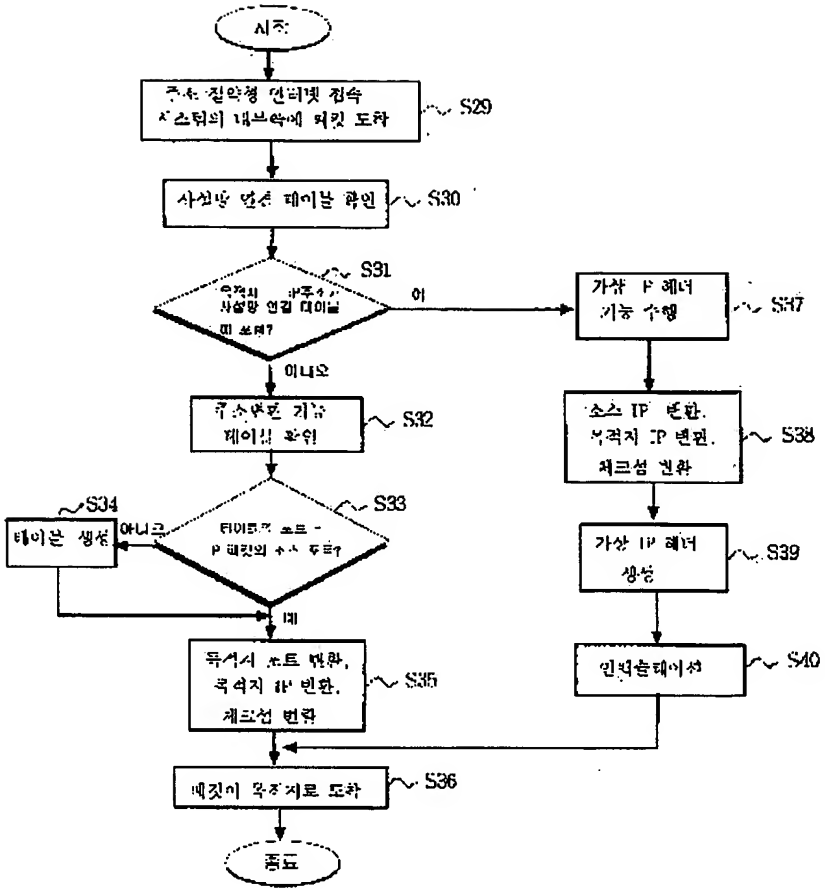



종래의 NAT 기능의 흐름도.

도면8



도면3



도면6